UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/576,516 | 05/23/2000 | Xin Qiu | 018926-002110US | 4301 |

43471 7590 10/23/2008

Motorola, Inc.
Law Department
1303 East Algonquin Road
3rd Floor
Schaumburg, IL 60196

| EXAMINER | |
|---|---|
| PYZOCHA, MICHAEL J | |
| ART UNIT | PAPER NUMBER |
| 2437 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 10/23/2008 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

Docketing.US@motorola.com

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/576,516 | QIU ET AL. | |
| | Examiner | Art Unit | |
| | MICHAEL PYZOCHA | 2437 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *05 September 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. Claims 1-19 are pending.

2. Response filed 09/05/2008 has been received and considered.

### *Claim Rejections - 35 USC § 103*

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al. (US 5870474) in view of Chen et al. (US 6324646).

As per claim 1, Wasilewski et al. discloses a method of providing varying levels of security in a data processing system, the method comprising: receiving information from an outside source; retrieving a first indicator from the received information that instructs the system to operate at a first level of security (i.e. a first encryption/decryption key) (see column 11 lines 10-23 where the MSK contains the decryption key for the encrypted content); continuing operation of said processing system at this level (see column 11 lines 10-23 and column 2 lines 53-67 where the processing continues until the user requests a different program); receiving further information from said outside source; retrieving a separate second indicator from said further information, the second indicator for instructing the system to operate at a different security level than the first indicator (see column 11 lines 10-23 and column 2

lines 53-67 where, when a user selects a different program, a different EMM is sent containing a different decryption key for the different program); receiving an encrypted message that authorizes the system to operate at the different level of security; authenticating the encrypted message (see column 11 lines 34-50); and preventing the operation at the different level of security until indicated by the second indicator and the encrypted message (see column 11 lines 10-50 where the program cannot be decrypted until the EMM is received and verified).

Wasilewski et al. fails to explicitly disclose that the second indicator received from the outside source instructs the system to move from a higher level to a lower level.

However, Chen et al. teaches including information from a source to vary the security level (see column 6 lines 6-43 and figures 4, 5, and 6 with their corresponding descriptions).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to change the level of security in Wasilewski et al. from a higher level to a lower level based on the indicator from an outside source.

Motivation to do so would have been to provide more flexibility in the security system (see Chen et al. column 6 lines 26-43).

As per claims 2-5, the modified Wasilewski et al. and Chen et al. system discloses a decreased security authorization code authorizing a decrease in the encryption/decryption levels and a decrease in the authentication level (see Wasilewski et al. column 11 lines 10-50 and Chen et al. column 6 lines 6-43).

As per claim 6, the modified Wasilewski et al. and Chen et al. system discloses wherein said encrypted message further comprises a key for use in a decryption algorithm (see Wasilewski et al column 11 lines 10-50).

As per claims 7 and 19, the modified Wasilewski et al. and Chen et al. system stores a master key (i.e. unique user key) to decrypt messages includes new decryption key values and using said master key stored at said system to decrypt said encrypted message (see Wasilewski et al. column 11 lines 10-50).

As per claim 8-12, the modified Wasilewski et al. and Chen et al. system discloses establishing a Security-Level-status-Indicator at said system to indicate a level of encryption/decryption and authentication that is being implemented (see Wasilewski et al. column 11 lines 10-50).

As per claim 13, the modified Wasilewski et al. and Chen et al. system discloses utilizing a cable head-end as said outside source including a set-top box (see Wasilewski et al. column 3 lines 43-52).

As per claims 14-17, the modified Wasilewski et al. and Chen et al. system discloses using a Key Management Message to convey said Decreased Security Authorization Code; wherein delivery of said Key Management Message is authenticated; wherein delivery of said Key Management Message is protected against a replay attack; wherein delivery of said Key Management Message is authenticated and protected against a replay attack (see Wasilewski et al. column 11 lines 10-50).

As per claim 18, the modified Wasilewski et al. and Chen et al. system discloses wherein a lower level of security is nonpublic Key mode, wherein a higher level of

security is a public Key mode, continuing operation of the system in the public Key mode until an encrypted predefined message is received by the system from the outside source (see Wasilewski et al. column 11 lines 10-50 and Chen et al. column 6 lines 6-43).

### *Response to Arguments*

5. Applicant's arguments filed 09/05/2008 have been fully considered but they are not persuasive. Applicant argues that Wasilewski and Chen do not include the claimed subject matter, particularly the following steps: "retrieving a first indicator from the received information that instructs the system to operate at a higher level of security;" "retrieving a separate second indicator from said further information.., for instructing the system to operate at a lower level of security than the higher level of security instructed by the first indicator;" "receiving an encrypted message that authorizes the system to operate at the lower level of security;" "authenticating the encrypted message;" and "preventing operation at the lower level of security until a decrease in security levels is indicated by said indicator and the encrypted message; while continuing operation of said processing system at the higher level of security"; and fail to teach the limitations of claims 2-5, 8-12, and 14-17.

With respect to Applicant's argument that Wasilewski and Chen do not include the claimed subject matter, particularly the following steps: "retrieving a first indicator from the received information that instructs the system to operate at a higher level of security;" "retrieving a separate second indicator from said further information.., for

instructing the system to operate at a lower level of security than the higher level of security instructed by the first indicator;" "receiving an encrypted message that authorizes the system to operate at the lower level of security;" "authenticating the encrypted message;" and "preventing operation at the lower level of security until a decrease in security levels is indicated by said indicator and the encrypted message; while continuing operation of said processing system at the higher level of security"; receiving information from an outside source; retrieving a first indicator from the received information that instructs the system to operate at a first level of security (i.e. a first encryption/decryption key) (see column 11 lines 10-23 where the MSK contains the decryption key for the encrypted content); continuing operation of said processing system at this level (see column 11 lines 10-23 and column 2 lines 53-67 where the processing continues until the user requests a different program); receiving further information from said outside source; retrieving a separate second indicator from said further information, the second indicator for instructing the system to operate at a different security level than the first indicator (see column 11 lines 10-23 and column 2 lines 53-67 where, when a user selects a different program, a different EMM is sent containing a different decryption key for the different program); receiving an encrypted message that authorizes the system to operate at the different level of security; authenticating the encrypted message (see column 11 lines 34-50); and preventing the operation at the different level of security until indicated by the second indicator and the encrypted message (see column 11 lines 10-50 where the program cannot be decrypted until the EMM is received and verified). Chen teaches including indicators in

messages to tell the receiving system which level of security to operate. At the time of the invention it would have been obvious to a person of ordinary skill in the art to change the level of security in Wasilewski et al. from a higher level to a lower level based on the indicator from an outside source. Motivation to do so would have been to provide more flexibility in the security system (see Chen et al. column 6 lines 26-43). Applicant contends that Wasilewski fails to teach changing any level of security because Wasilewski merely changes keys and one must change the encryption algorithm to change the security level. However, one of ordinary skill recognizes that keys have different strengths and therefore different levels of security. Applicant's specification even discusses using different keys for the different security levels (see pages 6 and 7). Applicant further states that Chen does not dynamically change the level of security. Wasilewski teaches such a dynamic changes in security while Chen was merely relied upon for the teaching of including an indicator in a message to state which security level the system should operate. When this is combined with Wasilewski the combination teaches such dynamic changing of security levels.

With respect to Applicant's argument that Wasilewski and Chen fail to teach the limitations of claims 2-5, 8-12, and 14-17, Applicant argues that because these references fail to teach the independent claim they could not teach these dependent claims. However, as discussed above Wasilewski and Chen teach the independent claims and therefore teach these claims as put forth in the rejection above. For example, the encrypted messages of Wasilewski including the indicator of Chen to lower the security correspond to the Decreased-Security-Authorization-Code which can

lower the encryption and/or authentication. Additionally, the indicator of Chen shows what level of security the system is operating at and therefore teaches the Security-Level-Status-Indicator. Finally, as stated above, the indicator of Chen is included in the messages of Wasilewski that change the security level of the system, in other words, the indicator of Chen is included in either the KMM or EMM messages of Wasilewski.

***Conclusion***

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Anderson teaches including an indicator of a security level in a KMM.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL PYZOCHA whose telephone number is (571)272-3875. The examiner can normally be reached on Monday-Thursday, 7:00am - 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/M. P./
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437